Proskauer Rose LLP Eleven Times Square New York, NY 10036-8299

Timothy Q. Karcher
Member of the Firm
d +1.212.969.4750
f +1.212.969.2900
tkarcher@proskauer.com
www.proskauer.com

May 23, 2025

By Email and ECF

Nan Roberts Eitel, Esq.
Associate General Counsel for Chapter 11 Practice
United States Department of Justice
Executive Office for United States Trustees
Office of the General Counsel
441 G. Street NW, Suite 6150
Washington, DC 20530

Re: *Berkeley Research Group Cybersecurity and Data Incident*

Dear Ms. Eitel:

We write in response to your letter dated May 6, 2025 (the "UST Letter") regarding the recent cybersecurity incident (the "Incident") at Berkeley Research Group, LLC ("BRG") and the notice that was filed in twelve chapter 11 cases (the "Subject Cases"), which describes the Incident in further detail (the "Incident Notice"). This letter has been prepared by BRG, Proskauer Rose LLP, and Octillo Law, PLLC.

Relatedly, BRG has also received written requests from parties involved in certain of the Subject Cases and is advising those parties that, to ensure everyone receives information in a consistent manner and due to the potential overlap in requests between those parties' letters and the UST Letter, we are providing this comprehensive response to the UST Letter in the Subject Cases, which will be shared with the relevant parties, and filed on the dockets in the Subject Cases.

As a preliminary matter, we wish to reiterate that BRG takes this matter very seriously. Our response has been robust and remains ongoing. We are cognizant of the importance of this issue to many varied constituencies – most importantly the individuals whose data may have been exposed – and will continue to work to provide transparency to the greatest extent possible under these unfortunate circumstances. While it has been mistakenly suggested that BRG believed that filing the Incident Notice would be its only post-Incident communication with stakeholders, nothing could be further from the truth. BRG has appeared, through counsel, at a number of status conferences in the Subject Cases and will do so at several more status conferences scheduled in the coming weeks. At each of these conferences BRG has informed, and will continue to inform, the courts and stakeholders that BRG, the victim of a serious and increasingly common crime, is committed to complying with all of its obligations. This includes, but is not limited to, complying with notice requirements and fulfilling its substantive obligations in the Subject Cases in the same manner as it has pre-Incident. BRG has also been in contact

with debtor's counsel in a number of Subject Cases and will continue its outreach without delay to the extent contact has not yet been established. BRG has been forthcoming with the information it has ascertained to date, and BRG will continue to provide information to the Office of the United States Trustee ("UST"), the courts, and the parties in the Subject Cases as its ongoing investigation progresses (including analysis of impacted data) and additional information becomes available. However, BRG respectfully notes that there is an active criminal investigation by the Federal Bureau of Investigation ("FBI") regarding the Incident that could restrict BRG from sharing certain information that might compromise the investigation or potentially incentivize similar cybercriminals to commit acts in the future against BRG or others. All affected constituencies share a common interest in locating and stopping the criminals that were responsible for this serious crime. BRG will continue to provide updates as additional information becomes available.

At the above-mentioned status conferences, BRG has noted four points of critical importance and reiterates them here for the benefit of those who were not present:

- The threat was discovered in March, and BRG took swift and decisive action, retaining cyber counsel at Octillo Law, as well as the incident response team at Booz Allen Hamilton to investigate, contain the threat, recover from the incident, and mitigate harm, including promptly engaging with the FBI.
- BRG reached a settlement with the threat actor after careful consideration and with a primary focus on protecting the subjects of any implicated data. As a result, BRG received a destruction log and a representation by the threat actor that any data exfiltrated during the Incident was deleted and will not be disclosed.
- Third, BRG has engaged experts to monitor the surface and dark web to detect the dissemination of impacted data. Those experts have not identified any information suggesting that the threat actor has breached its representation. Significantly, since the discovery of the Incident, more than two months ago, through the date of this letter, BRG has found no indication that any data that was potentially exfiltrated in the Incident has been distributed to anyone, and BRG has no reason to believe that the threat actor retained the data. BRG will continue to monitor the situation, including monitoring the dark web for the foreseeable future, and the FBI's investigation remains ongoing.
- The final point, which should be highlighted due to its significance, is that there is no indication that this crime was targeted at the data in the Subject Cases. The Incident affected data across BRG, including many clients and data having nothing to do with the Subject Cases, or any bankruptcy matter.

BRG's responses to the specific requests in the UST Letter are outlined below, but we first provide further explanation of BRG's actions in response to the Incident, as there are important clarifications to make at the outset (which also serves to address questions BRG has received from other parties in the Subject Cases).

First, one of the initial concerns raised in the UST Letter is the perceived inconsistency between the Incident Notice that was filed in the Subject Cases and the notice that was posted on BRG's website (the "Website Notice"). Separate from BRG's engagement in the Subject Cases, BRG also works with many clients who are Covered Entities under the Health Insurance Portability and Accountability Act ("HIPAA"). BRG is a HIPAA Business Associate because its Covered Entity clients provide BRG access to Protected Health Information ("PHI"). Early in BRG's investigation, it identified a potential impact to PHI from those clients, which could trigger a HIPAA requirement that notice be provided to individuals within sixty (60) days of discovery of the Incident. Based upon dialogue with the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") and the ongoing nature of BRG's data analysis, BRG posted the Website Notice to facilitate HIPAA compliance. This was an early disclosure – potentially required by HIPAA – at a time when BRG's investigation had not progressed to the point where it had a sufficient level of knowledge upon which to reasonably and responsibly commence a broader notice campaign.

The Website Notice was limited to the information known to BRG at the time it was posted and what was potentially required under HIPAA. As discussed in further detail below, BRG has not notified any impacted individuals because BRG is still in the process of analyzing the impacted data to identify such individuals. Nonetheless, by posting the Website Notice at this early stage, BRG has endeavored to provide useful information to any potentially affected individuals in line with its consistent, proactive approach throughout its response to the Incident.

To clear up any other misunderstandings on this point: it is, and always has been, BRG's intention to provide timely notification to individuals whose information was involved in the Incident (the "Affected Individuals"). The Website Notice will continue to serve as a placeholder in this regard, while BRG's ongoing data analysis focuses on identifying all Affected Individuals who require notice. BRG will timely comply with all statutory (and other) obligations, providing notice to those individuals directly, or through an appropriate alternative protocol. Relatedly, as it pertains to the information from the Subject Cases, BRG recognized at an early stage that the information requires additional care and sensitivity and, as such, the information is undergoing a more advanced data analysis in a prioritized manner with BRG's data analysis team. To that end, there are dedicated review teams who are conducting a digitally assisted and manual review of the entire population of impacted files associated with the Subject Cases. The reviewers have been instructed to record the presence of any information that could be associated with a person, regardless of whether the information equates to personally identifiable information under state data breach notification laws or other regulated data elements.

Another concern raised in the UST Letter, and in letters received from other parties in the Subject Cases, is the alleged delay between BRG's discovery of the Incident on March 2, 2025 and the timing of the distribution of the Incident Notices in the Subject Cases. There were numerous actions required before BRG could fully define the extent of the Incident and understand its impact, if any, on the Subject Cases. This process started during the week following discovery of the Incident, when the threat actor provided BRG with a file listing of the data it claimed to have taken and then subsequently provided copies of certain files from that list to BRG.[1] Following this development, BRG's information technology team had to undertake additional efforts to take this unstructured file list and restructure it into a usable, searchable format to conduct further analysis. This took time. Once that was complete, BRG's IT team conducted further analysis to attribute files of particular clients, law firms, and/or specific matters, where possible. One of the many issues BRG had to address was the fact that many of the file names did not say which matters they were associated with, while others may have had "project" names that did not reveal the name of the client, the BRG personnel, or the matter to which such files were related. Given that there was not an automated way to accomplish this task, BRG engaged in an enterprise-wide process of soliciting input from BRG experts to further confirm and identify whether files related to those clients, law firms, and/or specific matters. This feedback from BRG experts was then reconciled with the initial findings from BRG's IT team, to resolve any potential inconsistencies and compile a list of impacted matters tied to impacted clients and law firms.[2] Importantly, all these efforts occurred while BRG was engaged in negotiations with the threat actor, testing and deploying the threat actor's decryption tool to impacted BRG systems, reconstituting corrupted files, and conducting a full forensic investigation into the Incident.

BRG believed it was important that the Incident Notices be filed simultaneously. Throughout BRG's efforts outlined above, it also recognized that the risk of providing potentially incomplete or inaccurate information, with less clarity, on a faster timeline, was significantly outweighed by the benefit of developing a firmer, more accurate understanding of the impact to the Subject Cases and stakeholders before filing the Incident Notices. Providing information in a less thorough manner also risked causing unnecessary alarm to unimpacted clients and individuals given the sensitivity of the claims and information at issue in each of the Subject Cases.

BRG has undertaken a thorough and comprehensive process to understand the Incident's potential impact on the Subject Cases and stakeholders and BRG did not delay in providing the Incident Notice on the respective dockets. Instead, BRG moved as quickly as it reasonably could,

[1] BRG has received requests from other parties in the Subject Cases seeking production of this file listing. Given privilege and confidentiality restrictions based on the work product doctrine and proprietary business information relating to other BRG clients, as well as the confidentiality orders entered in the Subject Cases, BRG is unable to share this file listing with all parties involved in the Subject Cases.

[2] Notably, the reconciliation that BRG had to undertake in associating files to cases further illustrates that the threat actor was targeting BRG generally, not any specific client or matter.

while also ensuring that its process of scoping out the Incident's impact was commensurate with the degree of care and attention required in each of the Subject Cases.

Judge Grabill, at a recent status conference involving the Archdiocese of New Orleans, referred to the process outlined above as "triage" and her description is accurate. BRG has been engaged in a process of sorting information, in an emergency, to determine the order in which the information needs attention. The Subject Cases have consistently been prioritized. Having identified the files that were impacted, BRG has continued to engage a team of professionals to review each file and determine what information was contained in each file and what BRG must do to provide notice and further protections to individuals and entities whose data may have been involved.

BRG provides the foregoing narrative to assist all parties in their efforts to understand this Incident and the steps BRG has taken to address it, and we are available to discuss this matter further.

Additionally, responses to the specific requests in the UST Letter are set forth more fully below:

- Case name, number, and district of each known affected case.

  Response: **Based on BRG's investigation, the following is a list of affected cases involving sexual abuse claims in United States Bankruptcy Courts (the Subject Cases):**

Incident Letter Filed		
Case Name	**Case No.**	**District**
In re The Roman Catholic Bishop of San Francisco	23-30564	Northern District of California
In re Franciscan Friars of California, Inc.	23-41723	Northern District of California
In re The Roman Catholic Bishop of Oakland	23-40523	Northern District of California
In re The Roman Catholic Bishop of Santa Rosa	23-10113	Northern District of California
In re The Roman Catholic Bishop of San Diego	24-02202	Southern District of California
In re Roman Catholic Archbishop of Baltimore	23-16969	District of Maryland
In re Roman Catholic Diocese of Burlington	24-10205	District of Vermont

In re The Roman Catholic Church of the Archdiocese of New Orleans	20-10846	Eastern District of Louisiana
In re The Roman Catholic Diocese of Albany, New York	23-10244	Northern District of New York
In re The Roman Catholic Diocese of Ogdensburg, New York	23-60507	Northern District of New York
In re The Diocese of Rochester	19-20905	Western District of New York
In re The Roman Catholic Diocese of Rockville Centre, New York	20-12345	Southern District of New York

- Case name, number, and district of *other suspected* affected cases under BRG's review for a possible breach or cybersecurity incident.

  Response: **BRG has been engaged in several other cases that are not related to the diocese or archdiocese cases. In connection with such matters, BRG is in the process of notifying the clients and providing additional notices. BRG will provide this list to the UST, including the case name, number, and district, as requested. As noted above, BRG prioritized filing Incident Notices in the Subject Cases given the sensitivity of the claims and information at issue in them.**

  BRG further notes that Incident Notices were not filed in the following cases because, based on BRG's review to date, BRG understands that no data was exfiltrated that would warrant disclosure.

Case Name	**Case No.**	**District**
In re The Roman Catholic Diocese of Syracuse, New York	20-30663	Northern District of New York
In re Archdiocese of Milwaukee	11-20059	Eastern District of Wisconsin
In re Catholic Diocese of Wilmington, Inc.	09-13560	District of Delaware
In re Boy Scouts of America and Delaware BSA, LLC	20-10343	District of Delaware
In re The Diocese of Camden, New Jersey	20-21257	District of New Jersey
In re Roman Catholic Bishop of Great Falls, Montana	17-60271	District of Montana
In re The Roman Catholic Bishop of Stockton	14-20371	Eastern District of California

- Please explain whether BRG sent the "Incident Update" to every creditor in each case, or whether it only filed a single notice on the docket in each case.

  Response: **BRG has not provided notices to individual creditors at this time. BRG is in the process of identifying individuals whose personally identifiable information has been exfiltrated. BRG understands such notices may be required under various state laws (or other obligations). BRG notes the UST's use of the word "creditor" and further notes that notices may be required to parties other than creditors in the Subject Cases, but whose data was nevertheless exfiltrated. BRG will provide notices to such entities in accordance with any applicable obligations. BRG further notes, however, that there are sensitivities in these cases that may dictate the method of providing notice, and BRG has engaged and will continue to engage in discussions with the committees and debtors regarding the appropriate method to handle such notifications.**

- Please explain why BRG delayed two months between discovery and notice to the USTP and filing the "Incident Update" on the respective affected case dockets. BRG has admitted that it learned of the breach by March 2, and the USTP has now learned that there were some news reports as of March 6 about the breach.

  Response: **As noted above, BRG immediately undertook a thorough investigation to determine whether exfiltrated files related to the Subject Cases. The process was time consuming based on the manner in which the threat actor reported the file names to BRG. BRG was only able to provide notice after determining what the exfiltrated files related to, and whether exfiltrated files related to the Subject Cases.**

- Please explain what federal law enforcement agency(ies) BRG contacted after discovering the data breach, the method and timing of the notification, the name(s) of law enforcement contact(s), and the judicial district(s) where the report was made.

  Response: **Immediately after its discovery of the Incident, BRG contacted the FBI Cyber Division on March 3, 2025. BRG exchanged further communications with the FBI throughout BRG's investigation and negotiations with the threat actor. BRG is continuing its dialogue with the FBI and most recently met with the FBI on May 16, 2025. BRG recognizes that the UST has requested additional information, which BRG will provide directly to the UST in a secure manner, as BRG is concerned that revealing such information in this letter could compromise the efforts of law enforcement.**

- Please explain whether BRG, and not the respective estates, will cover the costs of the breach investigation and ransom payment and whether BRG will file sworn declarations on these issues.

  Response: **BRG does not intend to seek recovery of costs of the Incident investigation or ransom payment from the respective estates. As indicated above, BRG is investigating the Incident and will not charge the estates for the costs of such investigation.**

- Please explain whether BRG has an indemnification provision in its engagement agreements, and, if so, whether BRG waives all claims to indemnification from the estates for this breach.

  Response: **BRG is reviewing its engagements. BRG does not intend to seek indemnification from the estates for harms that were not caused by the estates or other estate professionals.**

- Please explain whether BRG has any insurance that covers cybersecurity incidents and data breaches.

  Response: **BRG has cyber insurance that has been engaged in response to this Incident.**

- Please explain what further remedies BRG will offer affected creditors or other parties. BRG admits that it is relying on the assurances of extortionists that the exfiltrated data was destroyed, yet BRG does not now know exactly what data was exfiltrated and what exactly it should be monitoring on the "dark web."

  Response: **In the event BRG's data analysis identifies the presence of creditors' names or other information in the exfiltrated data, BRG will be providing those individuals with formal notification and an offer of cost-free credit monitoring. Based on the results of the investigation, best practices, and guidance from counsel, BRG will also consider providing additional protections or other appropriate relief to individuals based on the findings from its data analysis. However, all the above obligations will be guided by the sensitivity of the data involved and the potential risk of harm. Accordingly, BRG recognizes that there may be special protocols necessary to provide remediation and protection, while also respecting the sensitive nature of the information.**

  BRG reports that there is no indication that any potentially exfiltrated data has been made available on the dark web. BRG has taken all available measures to prevent distribution of any data on the dark web. First, BRG reached a settlement

with the threat actor, which was facilitated, in part, in exchange for the actor deleting the data and producing a destruction log. However, BRG is not solely relying on the threat actor's representations that deletion has occurred. BRG has engaged cybersecurity specialists to conduct web monitoring, which includes monitoring the dark web, including data leak sites and forums where unauthorized actors are known to frequent or leverage, and further investigating various dark market forums to determine if any information related to the incident is being sold. Dark web monitoring at a more granular level is not possible at this time, given that BRG's data analysis is ongoing, but BRG plans to address this once that data analysis is complete, as the credit monitoring that will be offered to individuals will also include dark web monitoring specific to the individual and provide alerts to them if their information appears on the dark web.

Accordingly, BRG is providing dark web monitoring based on the information it knows at this time, and additional monitoring will be provided to the individuals, if they choose to enroll in such monitoring, once BRG has more information from its data analysis.

- Given [BRG]'s liability for any damages caused by these breaches, please explain why BRG does not now have a conflict of interest with its constituents in each of the affected cases that should result in BRG's disqualification and disgorgement or reduction of compensation as unreasonable given its admittedly compromised performance as financial advisor.

  Response: **BRG provides the following preliminary response to UST's questions regarding (1) disqualification and (2) disgorgement or reduction of compensation. BRG reserves the right to provide a more fulsome response should any party choose to seek any affirmative relief relating to these issues. As no such motion has been made, these questions are premature.**

  Nevertheless, BRG notes the following.

  The specific team at BRG working on the Subject Cases has been retained as Financial Advisor in multiple diocese and archdiocese cases, some of which have been ongoing for several years. BRG has been engaged in developing the advisory practice in connection with diocese and archdiocese cases since 2007, and over nearly two decades, BRG has established the preeminent advisory service practice for these types of matters. In addition, BRG professionals have been retained to provide advisory services in more than a hundred bankruptcy cases since BRG's inception. The team working on the diocese and archdiocese cases is not involved in the global response to the data Incident, other than in connection with the provision of notices and responding to the Incident in connection with the cases in which they are retained. As reported at the status conferences, the Incident is much larger than

just the Subject Cases, and BRG has no reason to believe the Subject Cases were the target of the crime.

Section 1103 of the Bankruptcy Code permits the committee to retain professionals to assist the committee. ("[The] committee may select and authorize the employment by such committee of one or more attorneys, accountants, or other agents, to represent or perform services for such committee.") 11 USC §1103(a).

Section 1103(b) provides that, "an attorney or accountant employed to represent a committee appointed under section 1102 of this title may not, while employed by such committee, represent any other entity having an adverse interest in connection with the case. Representation of one or more creditors of the same class as represented by the committee shall not per se constitute the representation of an adverse interest." 11 USC §1103(b).

Section 328 of the Bankruptcy Code provides "the court may deny allowance of compensation for services and reimbursement of expenses of a professional person employed under … 1103 of this title if, at any time during such professional person's employment under …. 1103 of this title, such professional person is not a disinterested person, or represents or holds an interest adverse to the interest of the estate with respect to the matter on which such professional person is employed. 11 USC §328(c).

The term "disinterested person" means a person that—"does not have an interest materially adverse to the interest of the estate or of any class of creditors or equity security holders, by reason of any direct or indirect relationship to, connection with, or interest in, the debtor, or for any other reason." 11 USC §101(14)(c).

Courts that have looked at the issue of potential disqualification of committee professionals in connection with 1103 involving an asserted adverse interest have looked at the totality of the circumstances. *See*, *In re Caldor, Inc. NY*, 193 BR 165, 172 (Bankr. SDNY 1996) ("most courts eschew a *per se* rule [relating to adverse interests] in favor of analysis premised on the totality of the circumstances in a particular case." In *Caldor*, the court allowed the retention of the committee's accountant, notwithstanding the accountant's simultaneous retention by a committee in the bankruptcy of a competitor to the debtor.

Here, disqualification is unwarranted because there is no disqualifying adverse interest in connection with the Subject Cases. BRG has not assumed any adverse interest to that of the estate or the creditors as a result of the Incident. *See* 11 U.S.C. § 101(14)(C). And indeed, case law suggests that Courts are unlikely to find that there is an adverse interest here. *See*, *e.g.*, *In re Leslie Fay Companies, Inc.*, 175 B.R. 525, 532 (Bankr. S.D.N.Y. 1994) (noting "interests are not considered 'adverse' merely because it is possible to conceive a set of circumstances under which they

might clash"). The Incident has created no "meaningful incentive [for BRG] to act contrary to the best interest of the [] Committee" that retained it. *In re Caldor, Inc. NY*, 193 B.R. 165, 171 (Bankr. S.D.N.Y. 1996) (quotations and alterations omitted). BRG has no incentive "to place [the] parties at more than acceptable risk" as a result of the Incident. *Id.* And the facts of the Incident do not give rise to any "reasonable perception" of any such incentives. *Id.* Further, there are a number of entities who are in the same position as the creditors in the Subject Cases with respect to BRG in connection with the Incident, and those entities have nothing to do with the Subject Cases. In other words, the theft of the data is not "in connection with the" Subject Cases, and the Incident involves many entities who have no connection with the Subject Cases.

In *Caldor*, the court found that the party seeking disqualification was misreading 1103(b), and that their interpretation of the statute "effectively reads the phrase 'in connection with the case' out of section 1103(b), leaving only consideration of whether an adverse interest exists." 193 B.R. at 175. BRG believes the UST may be doing the same here.

Further, BRG's interests—as it relates to the Incident—are aligned with the constituents in the Subject Cases, including those of the estates. And its current primary interest continues to be ensuring that no harm comes to any constituents of the Subject Cases (or any of the individuals whose information may have been exposed) as a result of the Incident. Thus, BRG maintains it is a "disinterested person" as defined by 11 U.S.C. § 101(14)(C). Accordingly, 11 U.S.C. § 1103(b) does not warrant disqualification.

Second, disgorgement of profits and reduction of compensation are also unwarranted. BRG respectfully notes the UST does not specify the statutory, regulatory, or factual basis for such a disgorgement or reduction of compensation. However, BRG maintains that it was, and remains, a disinterested person at all times and did not hold or represent any interests adverse to the interests of the constituents of any of the affected cases with respect to the matters on which it is employed. *See* 11 U.S.C. § 328(c). BRG also notes that the language of section 328 is permissive, not mandatory. Accordingly, BRG respectfully submits that there is no basis for either disgorgement or the withholding of compensation under 11 U.S.C. § 328(c). Importantly, BRG's performance as a financial advisor was not affected by the Incident and BRG remains fully able to perform the functions for which it has been retained. Indeed, disqualifying BRG in connection with this crime would impose cost, delay, and other burdens associated with replacing it as the financial advisor in a dozen or more active chapter 11 cases. Accordingly, there is no basis or reason for disgorgement or reduction of compensation.

Additionally, the premise of this inquiry requires us to address the issue of liability. First, BRG respectfully rejects any suggestion of liability. BRG was the victim of the

ransomware attack, not the perpetrator. To reiterate – BRG was the victim of a crime. That crime is being investigated by the Department of Justice. There is no evidence that BRG should be penalized for the Incident caused by the criminal threat actor and certainly the UST Letter does not explain why the UST believes liability should attach. Critically, and to avoid all doubt, BRG maintains that it had—at all times—reasonable and adequate security measures in place. The fact that the Incident happened is not—by itself—a basis for liability. *See, e.g., Hummel v. Teijin Auto. Techs., Inc.*, No. 23-CV-10341, 2023 WL 6149059, at *5 (E.D. Mich. Sept. 20, 2023) (declining to "infer the breach of duty from the mere existence of the Cyberattack" because it "would, in effect, create strict liability in data breach cases"). There is no basis to suggest BRG should be liable for damages simply because it fell victim to a criminal ransomware attack (as have so many other organizations, including organizations involved in these and other bankruptcy cases) and such an assertion would be contrary to well established law.

Second, BRG rejects the notion that there are currently any damages for which BRG could be liable. Indeed, BRG is not currently aware of any evidence that the Incident has caused actual damages for anyone other than BRG. Nor is there currently any evidence that the attacker targeted particular data or intended to harm anyone other than BRG.

Lastly, BRG rejects the notion that BRG's performance as a financial advisor has been "admittedly compromised." Not only has BRG never made such an admission, but BRG is also not even aware of any such claim by any of the constituents of any of the Subject Cases. Rather, despite being the victim of the Incident, BRG's performance as a financial advisor is a separate matter and remains unaffected.

- Given the confidentiality orders entered in many of these cases, please explain why BRG should not be liable for sanctions for violating them.

  Response: **The UST Letter does not identify any specific provision of any confidentiality order(s) that were purportedly violated by BRG, and BRG respectfully does not have sufficient knowledge of the concerns of the UST to meaningfully respond to the suggestion that sanctions would be inappropriate.**

  BRG recognizes, however, that the various confidentiality orders ("Orders") entered in each case generally prohibit a Receiving Party from disclosing or using any material designated as confidential except as authorized by the Orders. However, as BRG has explained, BRG was the *victim* of a ransomware attack. Although it is deeply regrettable the threat actor gained unauthorized access to information involved in the Subject Cases, BRG did not disclose any such information to the threat actor in violation of any Orders. Accordingly, BRG respectfully rejects the notion that any of its conduct warrants sanctions.

The Orders do not prohibit the recipient of confidential information from falling victim to a crime. Nor do any Orders require a recipient to have impenetrable security—as that would be impossible. In fact, many of the Orders do not mention data security at all. Nevertheless, as noted above, BRG had reasonable and adequate security measures in place to protect the information involved in the Subject Cases.

One of the central functions of a Protective Order is to protect the disclosure of material to other parties involved in the cases who would not otherwise be entitled to view such material because of confidentiality concerns or otherwise. Here, there was no disclosure to *any other party* to these cases.

Our sincere hope is that the information provided above will serve to clear up any misunderstanding regarding BRG's response to the Incident and future intentions. We also look forward to the opportunity to meet with you and your colleagues to discuss any lingering questions or concerns as we continue to work through the issues identified above.

Respectfully,

Timothy Q. Karcher

cc: United States Trustees and Assistant United States Trustee on Subject Cases
Committee Lead Counsel for Subject Cases
Debtor Lead Counsel for Subject Cases
Court Dockets for Subject Cases